1   TRIAL & TECHNOLOGY LAW GROUP
    A PROFESSIONAL CORPORATION
2   ROBERT A. SPANNER SBN 60308
3   3723 HAVEN AVENUE, SUITE 132
    MENLO PARK, CA 94025
4   PHONE:/(650) 324-2277
    FAX: (650) 324-0178
5   email - ras@techtriallaw.com

6

7

8   Attorney for Plaintiffs

9   **UNITED STATES DISTRICT COURT**

10   **NORTHERN DISTRICT OF CALIFORNIA**

11   **San Francisco Division**

12

13

14 HENRY A. KLYCE and CAROLE M.   CASE NO. 11 CV 02248 WHA
    KLYCE,

15   **PLAINTIFFS' *EX PARTE***
                                            APPLICATION FOR LEAVE TO TAKE
16   Plaintiffs,   **EXPEDITED DISCOVERY AND**
                                            APPLICATION FOR ORDER ON
    v.
17   **SHORTENED TIME FOR**
    DOES 1-10,   **IMMEDIATE ASSIGNMENT TO A**
18   **MAGISTRATE**
            Defendants.
19 _____/

20   **EX PARTE APPLICATION FOR LEAVE TO TAKE EXPEDITED DISCOVERY**

21   This case involves an illegal Internet scheme, in which the identity of the actual

22 defendant is unknown and must be discovered. Plaintiffs bring this motion for expedited

23 discovery pursuant to F.R.Civ.P. 26(f) in order to ascertain the identity of Defendant Doe One

24 so that he or she may be served with process; they bring this motion *ex parte* because they do

25

26 not yet know his or her identity.

27 _____
    Mot. to Expedite Discovery and Shorten Time
28 Case No. 11 CV 02248 WHA
                             1

Plaintiff Henry Klyce is a successful serial entrepreneur, having founded and sold four medical device companies. He and his wife, Carole Klyce, allege causes of action for: 1) violation of the Computer Fraud and Abuse Act, 18 U.S.C. §1030, as well as its state-law counterpart, the Comprehensive Computer Data Access and Fraud Act, Cal. Pen. Code §502(c)(1); 2) e-personation under Cal.Pen. Code §528.5; and 3) the Stored Communications Act, 18 U.S.C. §2701 *et. seq.* There is also a §17200 claim based on the foregoing unlawful acts.

Plaintiff Carole Klyce has her email account with Internet Service Provider ("ISP") Yahoo!; Henry Klyce has an AOL email account. In essence, Plaintiffs allege that they have been victimized by an Internet predator, who has undertaken all manner of malicious mischief in connection with their respective email accounts. This person has:

1) deprived them of access to their email accounts (Complaint, ¶7-8);

2) deleted their email, and sometimes whole email folders (Complaint, ¶9);

3) impersonated them by sending offensive and malicious emails from Carole Klyce' email account to their family and friends (whose identities the predator had learned of by reading Carole Klyce' email), causing the recipients great anguish and Ms. Klyce humiliation and emotional distress (Complaint, ¶10);

4) changed Ms. Klyce' password information so that she could not exclude the predator from her email account by changing her password (Complaint, ¶11); and

5) set up a phony email account under the name klycehenry@yahoo.com and initiated mass mailings in Mr. Klyce' name to insurance companies and college admissions offices, resulting in a deluge of solicitations (Complaint, ¶12).

_____

Plaintiffs seek the IP address of the predator. According to Plaintiff's expert, who has many years of experience in computer and Internet investigations and is currently a security employee at Yahoo! (Seiden Decl., ¶¶1-4), each time a person logs into an email account, that person's IP address is automatically recorded by the email service provider servicing the account (Seiden Decl., ¶8), and is stored for a period of time. Therefore, the predator who has been logging into Carole Klyce' email account, and the person who set up the "klycehenry@yahoo.com" account, left an electronic fingerprint – an IP address. However, the IP address of each person logging into Plaintiffs' Yahoo! or AOL email accounts is not actually available to them – even though it is their accounts which were invaded. The ISP's require a court order in order to release documents pertaining to an individual's account – not even a subpoena is sufficient (Seiden Decl., ¶9), due no doubt to concerns about statutory account confidentiality in the Cable Communications Policy Act, 47 U.S.C. §551(c)(2)*; see, e.g., Liberty Media Holdings, LLC v. Does 1-59*, 2011 U.S. Dist. LEXIS 7563, *2 (S.D. Cal. Jan. 25, 2011).

From the predator's IP address one can determine which ISP is servicing the predator's email account[1]. That ISP can then be subpoenaed for the identity of the person with the known IP address. Plaintiffs also seek documents reflecting the identity of the person who created and exercised control over the aforementioned "klycehenry" email account at Yahoo! Accordingly, this Court is respectfully requested to issue an order substantially in the form of the Proposed

---

[1]   The intruder's own ISP (*i.e.,* the company which is providing email services to him or her) can be identified from the intruder's IP address (Seiden Decl., ¶10), and then documents can be subpoenaed from that ISP for the intruder's physical identity (*id.*).

_____
Mot. to Expedite Discovery and Shorten Time
Case No. 11 CV 02248 WHA

3

1   Order submitted herewith, which not only identifies the documents sought but also makes

2   allowance for the legitimate rights of the ISP and Defendant Doe One.

3   While discovery usually must await the parties' Rule 26(f) conference, Rule 26(d)

4   provides for earlier discovery "for the convenience of parties and witnesses and in the interests

5   of justice." The standard for such expedited discovery is "good cause". There is eminent good

6   cause for expedited discovery in this case, for the purpose of identifying the Doe Defendant(s)

7   (presently identified as "Does I -X"), for without such discovery Plaintiffs obviously cannot

8   proceed with their lawsuit because they cannot serve the Complaint. In this Circuit," where the

9   identity of the alleged defendant[] [is] not [] known prior to the filing of a complaint[,] the

10 plaintiff should be given an opportunity through discovery to identify the unknown

11 defendants." *Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999), *citing Gillespie v.*

12 *Civiletti,* 629 F.2d 637, 642 (9th Cir. 1980).

13   Cases such as this one – involving tortious or unlawful conduct committed over the

14 Internet – often require expedited discovery from the perpetrator's and victim's Internet Service

15 Providers in order to discover the perpetrator's identity before the time to serve process runs

16 out. Judges in this District apply the four-factor analysis set forth in *Columbia Ins. Co. v.*

17 *Seescandy.com*, 185 F.R.D. 573, 578-80 (N.D. Cal. 1999) to assess the reasonableness of such

18 a request[2]:

19   1) is there an identification of steps taken to locate the unidentified defendant;

20   2) has the absent defendant been described with sufficient specificity to be assured that

---

[2] The order has been re-arranged for coherence.

1   the defendant is a real person or entity susceptible to process in Federal court;

2   3) has the applicant has set forth a justification for the specific discovery requested, and

3   is there a reasonable prospect that that discovery, from a limited number of persons or

4

5   entities, will lead to the identification of the absent defendant so that service can be

6   effected;

7   4) are the claims against the absent defendant sufficient on their face.

8   Applying the four-factor test adopted in this District, "good cause" is clearly present here –

9   especially in light of the fact that, because of its volume, ISP's retain log-in data – the kind of

10

11   information sought here – for only limited periods (Seiden Decl., ¶12), so that if discovery is

12   delayed until a Rule 26 Conference is held, the evidence may no longer be available[3]:

13   First, Plaintiffs have set forth what steps they have taken to identify the perpetrator of the

14   misdeeds, and they have identified the miscreant with as great a specificity as the circumstances

15   and the law presently permit. Carole Klyce called in Yahoo! Security to identify who had seized

16   control of her email account, and Yahoo! personnel did conduct an investigation of her account

17

18   (Seiden Decl., ¶7). However, Yahoo! will not disclose anything about the account (including

19   what IP addresses were accessing the account without authorization) until a court order for

20   disclosure of that information has issued (Seiden Decl., ¶9). Similarly, an Internet security

21   expert also determined that Henry Klyce' AOL email account had been tampered with (Seiden

22   Decl., ¶7), but his ISP – AOL – will not disclose further identifying information about the

23   tamperer without a court order either (Seiden Decl., ¶7).

24

25

26   [3]   Moreover, no Rule 26 Conference can even be held until the Defendant has been
     identified and served.

27

     _____
28   Mot. to Expedite Discovery and Shorten Time
     Case No. 11 CV 02248 WHA

                                           5

Second (and third), an order for issuance of the subpoena by the Court is likely to lead to the identification of the Defendant perpetrator and to the service of process upon him. There is an identity between the person whose IP address appears in the log-in information for Carole Klyce' email account at Yahoo! and Henry Klyce' email account at AOL and the person who committed the above-referenced offenses. Similarly, there is an identity between the perpetrator of the harassment of Henry Klyce and the person with the IP address that set up the klycehenry.com email account. Thus, issuance of the requested court order will result in the unveiling of the perpetrator.

Fourth, the allegations of the Complaint clearly state claims for relief that would survive a motion to dismiss:

Stored Communications Act (First Cause of Action): The Stored Communications Act, 18 U.S.C. §2701(a)(1) prohibits unauthorized access to an electronic communications service, and §2701(a)(2) prohibits anyone from obtaining, altering, or preventing authorized access to a wire or electronic communication while it is in electronic storage. Plaintiffs allege that their ISP was a stored communications service within the meaning of the statute, that the Doe defendants accessed Yahoo! computers without authorization, that Plaintiffs' account was unlawfully accessed and they themselves were denied access, and that their electronic communications were altered, all to their injury (Complaint, ¶¶7-14, 16-18).

Computer Fraud and Abuse Act (Second Cause of Action): The Computer Fraud and Abuse Act, 18 U.S.C. §1030(a)(5)(A) makes it unlawful to" knowingly cause[ ] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer". Plaintiff alleges that the

_____
Mot. to Expedite Discovery and Shorten Time
Case No. 11 CV 02248 WHA

6

predator accessed Yahoo!'s computers without authorization, and thereupon loaded software or commands which enabled them to seize control of Plaintiffs' email accounts, thus enabling them to block Plaintiffs' access, destroy Plaintiffs' files, and impersonate Plaintiff Carole Klyce by sending email from her account to her friends and family (Complaint, ¶¶8-10, 24-25).

Comprehensive Computer Data Access and Fraud Act (Third Cause of Action): This statute, Cal. Pen. Code §502(c)(1) *et. seq.*, states that anyone who "knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to . . . (A) devise or execute any scheme or artifice to defraud" is guilty of an offense. As noted above, Plaintiffs alleged that the intruder accessed Yahoo! computers and their account without authorization, and then altered and damaged their files. They also allege that the Doe defendant executed a scheme to defraud by impersonating Carole Klyce and sending emails from her account to her family and friends. In doing these acts, the Doe defendant also violated § 502(c)(2), which makes it unlawful to knowingly access and without permission take, copy or make use of any data from a computer; and §502(c)(4), which makes it unlawful to knowingly access and without permission to alter, damage, delete, or destroy any data on a computer. The absent defendant altered and damaged the data on Carole Klyce' computer by deleting her email files, and altered Henry Klyce's account security information (Complaint, ¶¶29-34)[4].

E-Personation Statute (Fourth Cause of Action): California just passed Pen. Code §528.5, which prohibits impersonation on the Internet. By sending emails from Carole Klyce's

---

[4] Indeed, Doe's conduct violated five independent provisions of the statute.

_____
Mot. to Expedite Discovery and Shorten Time
Case No. 11 CV 02248 WHA

7

1   account, the Doe defendant made her friends and family believe Carole Klyce herself had sent

2   them (Complaint, ¶¶41-42), thus violating the statute.

3   **Section 17200 Claim** (Fifth Cause of Action): The California unfair competition statute

4   was also violated (the "unlawful" prong) once any of the foregoing statutes were violated.

5   **Summary**: It is evident that the Plaintiffs have stated claims which would survive a

6   motion to dismiss.

7

8   In the Northern District of California – which is home to so many Internet companies –

9   good cause for expedited issuance of a subpoena to an ISP to discover a miscreant's identity has

10 invariably been found; *see, e.g., Solarbridge Tech. v. John Doe*, 2010 U.S. Dist. LEXIS 97508,

11 at *3-4 (N.D. Cal. Aug. 27, 2010); *IO Group, Inc. v. Does 1 - 435*, 2011 U.S. Dist. LEXIS

12 14123, *2 (N.D. Cal. Feb. 3, 2011); *Zoosk Inc. v. Doe*, 2010 U.S. Dist. LEXIS 134292, *4-6

13 (N.D.Cal. 2010); *see also Liberty Media Holdings, LLC v. Does 1-59*, 2011 U.S. Dist. LEXIS

14 7563, *3-8 (S.D. Cal. Jan. 25, 2011). Accordingly, an order should issue authorizing service of

15 subpoenas upon Yahoo! in accordance with the Court's direction. A Proposed Order

16 accompanies these motion papers.

17

18   **MOTION FOR ORDER SHORTENING TIME**

19

20   In light of the fact that the instant motion pertains to discovery, it will presumably be

21 referred to a magistrate judge. Because of the ongoing destruction of log-in information (the

22 incriminating "fingerprint") by ISP's, this Court is urged to make that assignment as soon as is

23 practicable; and Plaintiffs further urge that upon reassignment of the matter, the responsible

24 magistrate judge set a hearing on shortened time, or resolve the motion promptly without

25 argument at the Court's earliest convenience.

26

27 _____
    Mot. to Expedite Discovery and Shorten Time
28 Case No. 11 CV 02248 WHA

1   Dated: May 23, 2011   Respectfully submitted,

2   TRIAL & TECHNOLOGY LAW GROUP
3   Attorneys for Plaintiffs
                                            CAROLE AND HENRY KLYCE
4

5   /s/ Robert A. Spanner
                                            By _____
6   Robert A. Spanner

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27   _____
      Mot. to Expedite Discovery and Shorten Time
28   Case No. 11 CV 02248 WHA